Written Testimony of Nicholas Andersen

Before the House Judiciary Committee

Subcommittee on Courts, Intellectual Property, and the Internet

Hearing: “Protecting Our Edge: Trade Secrets and the Global AI Arms Race”

May 7, 2025

Chairman Issa, Ranking Member Johnson, and distinguished members of the Subcommittee, thank you for the opportunity to testify on the urgent matter of protecting American trade secrets in the age of artificial intelligence (AI).

My name is Nicholas Andersen. I previously served as a senior cybersecurity official during the Trump administration, including as the Principal Deputy Assistant Secretary and Performing the Duties of the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response at the United States Department of Energy, in addition to my service in the White House, as a State Chief Information Security Officer (CISO) and Intelligence Community Chief Information Officer (CIO).

Today, I appear before you not as a legal expert as many of my colleagues may be, but as a national security and cybersecurity professional who has spent nearly two decades defending the United States against digital threats—many of them originating from the People's Republic of China (PRC). We are engaged in a global competition, and at its heart is the ability to secure and control the most advanced technologies of our time. Artificial intelligence is not merely an economic driver—it is a battlefield asset.

During the previous Trump administration, we delivered historic progress on securing critical energy infrastructure, elevating federal and private-sector collaboration, and taking unprecedented steps to disrupt cyber operations by adversaries. We prioritized real-world outcomes over bureaucratic exercises, and it worked. That results-driven approach must return again as we now commit again to outcomes rather than soundbites.

Unfortunately, over the past four years, we have watched strategic deterrence erode. Foreign adversaries face fewer consequences for targeting American innovation. Executive branch agencies have been more focused on process than protection. We must be prepared to act decisively and without hesitation to confront this threat.

The Chinese Communist Party (CCP) sees AI as a foundational element of its effort to supplant the United States as the global technological, economic, and military leader. Their strategy is not just to build capabilities domestically, but to extract, acquire, and steal them from us—through cyber-enabled theft, insider infiltration, and coerced transfer of technology. For China, innovation theft is not just tolerated—it is systematized, state-sponsored, and celebrated.

We must treat this for what it is: a sustained, government-backed assault on the American innovation base. The PRC is not operating as a competitor in good faith. They are leveraging their intelligence services, their state-owned enterprises, and even American legal and financial institutions to create openings for espionage and exploitation. And they are doing it in real time.

What makes the PRC threat uniquely dangerous is not just the scale of its cyber operations, but the strategic doctrine behind them. The CCP's Military-Civil Fusion policy erases any distinction between the private sector and the Chinese military. Their National Intelligence Law requires all citizens and entities to cooperate with state intelligence activities upon request. This means that any Chinese company interacting with American firms—whether through investment, supply chain participation, or joint research—is potentially an extension of the Chinese state.

In the cybersecurity community, we have long recognized that trade secret protection is only as strong as the defensive perimeter surrounding the data. Unlike patents, trade secrets are not protected by legal registration, but by the integrity of the systems, networks, and people that guard them. For this reason, cyber-enabled espionage is the single greatest threat to the long-term viability of American AI development.

The tactics used by the PRC and its proxies are wide-ranging: from remote intrusions targeting source code repositories and research institutions, to the use of joint ventures and academic exchanges as cover for data extraction. These efforts are deliberate, persistent, and operationally supported by the Chinese intelligence and military apparatus. It is not a matter of if they are targeting us—it is a matter of how deeply they have already penetrated key sectors.

From a national security standpoint, we must treat AI companies—especially those working in dual-use applications—as critical infrastructure. Their models, training data, and research pipelines are not just business assets; they are targets of foreign intelligence collection. Congress should act with urgency to prioritize cyber hardening measures across this sector. This includes developing minimum cybersecurity requirements for firms operating in designated strategic technology areas, expanding access to classified threat intelligence, providing incentives for robust secure-by-design practices, insider threat detection programs, and participation in classified or unclassified threat-sharing programs operated by the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI).

Additionally, we must recognize that our adversaries do not only exploit our networks—they exploit our openness. American capital itself can be a vector for strategic vulnerability. Private equity and venture capital firms—many of which are headquartered in the United States—routinely fund startups or firms operating in critical technology sectors without fully understanding or disclosing the downstream national security risks. They become unwitting participants in China's acquisition strategy. Congress should move swiftly to codify outbound investment screening mechanisms, restrict engagement with entities affiliated with the CCP and the Chinese military, and to require public disclosures of investments that involve AI or other sensitive technologies when there is a nexus to foreign ownership or influence.

We need a new doctrine for cybersecurity and AI—a clear, uncompromising framework built on American strength. It must include: zero taxpayer dollars for tech that strengthens China, no federal contracts without real standards for adequate cybersecurity, no more U.S. capital funding adversary-controlled firms, and a decisive offensive cyber posture to disrupt and dismantle threat actor infrastructure before harm occurs.

There is a narrative that stronger protections or tougher cyber requirements will somehow “slow down” innovation. I believe the opposite is true. Failing to protect what we build is what truly limits our future. American innovation thrives when our best minds and companies know their work will not be stolen, cloned, or militarized against them by a foreign regime.

I would caution this Subcommittee against overreliance on legal mechanisms alone. Laws and lawsuits do little good when the adversary operates outside our jurisdiction and beyond the reach of our courts. We need preemptive action, not passive defense. We must build resilient networks, promote real-time threat sharing, empower private sector defenders, and coordinate disruption efforts against foreign cyber actors. This must be a whole-of-government and whole-of-nation response.

The clock is ticking. Based on the pace of Chinese technology acquisition, the growing capabilities of its cyber operations, and the accelerating role of AI in defense and intelligence, I believe we have no more than two to five years to close the most dangerous gaps. Failing to act now will result in the permanent erosion of our technological and strategic advantage.

American companies developing AI systems are being targeted systematically. The tactics used by PRC-linked actors include cyber intrusions, insider recruitment, investment strategies meant to gain access to non-public information, and partnerships with academic institutions designed to extract sensitive research. Recent indictments by the United States Department of Justice (DOJ) and ongoing reporting by the ODNI confirm the breadth and sophistication of this campaign.

Protecting America’s AI future is not about isolationism or fear—it is about clarity, discipline, and courage. We must recognize that AI is not just a competitive industry: it is a foundation of national power. We must treat it accordingly.

Thank you for the opportunity to share my perspective. The United States cannot afford delay. We need leadership that understands this threat, has countered it firsthand, and will not hesitate to act. I stand ready to serve.

In the coming years, the United States must make a conscious decision about what kind of leadership it wants in the cyber domain. We can either remain on defense, reacting to breaches and intellectual property theft after the damage is done—or we can lead again.

Leadership means unapologetically defending American interests. It means re-establishing global norms through strength, not submission. It means calling out adversaries by name—especially the People's Republic of China—and holding them accountable with real costs, not symbolic gestures.

We need a return to the kind of decisive, disruptive cyber posture we began building in 2017. That includes stronger public-private partnerships, bold offensive capabilities, and the institutional will to act faster than our adversaries.

Thank you again for this opportunity to contribute to our national dialogue. I look forward to answering the questions of this Subcommittee as we seek to restore American strength in the digital age.